The Improved Cloud Computing Adoption Framework to deliver secure services

Muthu Ramachandran[1], Victor Chang[1], Chung-Sheng Li[2]
1. School of Computing, Creative Technologies and Engineering, Leeds Beckett University, Leeds LS6 3QS, UK.
2. IBM Thomas J. Watson Research Center, Yorktown Heights, NY 10598, USA
{M.Ramachandran;V.I.Chang}@leedsbeckett.ac.uk; csli@us.ibm.com

Keywords: Cloud Computing Adoption Framework Update (CCAF 1.1), Cloud security, Framework for Cloud

Abstract: This paper describes a high-level approach for our improved Cloud Computing Adoption Framework update 1 (CCAF 1.1), which emphasizes on the security policies, recommendations, techniques and technologies to be updated in our framework. Motivation, background, security overview and recent attack methods have been discussed. We propose a solution based on arising needs to improve current Cloud security, Fine Grained Security Model (FGSM) which is designed to integrate three different types of security methods and offer multi-layered security for a better data protection. Technologies and techniques behind FGSM have been explained and will be useful for our CCAF 1.1 development.

1 INTRODUCTION

Cloud Computing has transformed many organizations in several ways. First, organizations can consolidate the infrastructure, since the deployment of virtual machines can replace the use of physical machines. While there are less computers, people and spaces being used, this helps organizations reduce the operational costs in the long-term. An alternative for small and medium businesses is to outsource their services to other vendors to reduce costs (Khajeh-Hosseini et al, 2010; Weinhardt et al., 2009;). Second, less carbon and wastes will be produced due to the scale down of servers, air-conditioning systems and spaces. In this way, Cloud Computing supports Green IT and sustainability to cut down energy and resource wastes (Khajeh-Hosseini et al, 2010; Marston et al, 2011). Third, Cloud Computing can streamline business processes at some organizations. For example, it takes less time and effort to find goods, package and deliver for supply chain service providers when orders have been received. This improves their work efficiency, since some operational tasks can be completed quicker with better (Marston et al, 2011). Fourth, Cloud Computing offers offers companies more business opportunities since they can work as service providers and can access wider groups of customers based in different parts of the country or the world (Weinhardt et al., 2009; Marston et al, 2011). Fifth, Cloud Computing can provide a platform for scientists and developers to use and share their code (Velte et al., 2009). They make use of libraries and APIs to directly interact on the Cloud. However, there are challenges such as security, data ownership and bottle neck to performance and services (Armbrust et al., 2010). Apart from all these challenges, different organizations have used Cloud Computing for different purposes. For example, Company A uses Cloud Computing for outsourcing since they outsource their servers to the vendors. Company B uses Cloud Computing to facilitate their demanding services. So at their peak hours, they use Cloud Computing to share the workload so that more tasks or requests can be completed quickly. Company C uses Cloud Computing to improve work efficiency by completing more workloads at the same time and they can reduce resources including human resources. Company D uses Cloud Computing to store all their experimental data in the Cloud so that they can use it whenever they have access to the internet. Company E use Cloud Computing so that all their office documents and orders are completed, processed and stored in the Cloud and they work as a mobile office as a service. Company F offers Cloud Computing as a Consulting as a Service to help their clients develop infrastructure, platform and software according to their clients' need. Although security challenge applies in these six companies, the challenges that all six companies are facing, will require processes,

recommendations and guideline to help them achieve their goals and objectives. In other words, they need a well-structured, proven and well-established framework to guide and help them achieve their goals, improves their efficiency, increase their business opportunities and teamwork, reduces errors and rate of failures. The development of a framework that takes challenges and resolution into considerations is highly recommended and should always be encouraged.

1.1 Overall Discussion about Cloud Computing Adoption Framework

There are researchers attempting to illustrate the framework approach for Cloud Computing best practices. Low et al (2011) describe how their Technology, Organization and Environment framework can be used and developed as their Cloud adoption framework. They used qualitative approach and sent out questionnaires to directors and decision-makers in Taiwanese firms. Based on their analysis, they validate their hypotheses. However, such an approach appears to be applicable to Taiwan and their proposal is not entirely adopted by other organizations in other countries. Khajeh-Hosseini et al (2010) present a case study and demonstrate a work similar to a framework level. They explain the strengths and weakness of adopting Cloud Computing and ways to reduce costs and improve efficiency. However, their work is not a framework addressing specific and general problems. They do not have comprehensive guidelines to help organizations at different levels of adoption rather than focusing on calculations of cost-involved in Cloud Computing adoption.

IBM (2010) has developed their IBM Cloud Adoption Framework to advise the best approaches and recommendations while developing services in different types of Clouds at the time of publication. They use diagrams to illustrate their concepts. However, there is a lack of real-life case studies to support their vision and points of views. This explains why a collaboration with independent researchers is helpful for Cloud Computing research. Chang and Li (2012) et al have started the first collaboration to demonstrate the first prototype of Financial Software as a Service (FSaaS) and illustrate FSaaS can be ported to different types of Clouds with its performance benchmark tested. More research outputs have been updated from Year 2012 onwards. Chang et al (2013 a) and Chang (2015) propose their Cloud Computing Business Model (CCBF) which has four major components and compiles a summary of successful deliveries and case studies of Cloud Computing. There are reported added value and benefits from organizations that have adopted Cloud Computing under the guidelines of CCBF. Selected results have been presented in their papers. However, there is no detailed information from the design to implementation to service delivery. Due to this reason, the next phase of work known as Cloud Computing Adoption Framework (CCAF) has been developed (Chang et al, 2013 b; Ramachandran and Chang, 2014). CCAF emphasizes more on the practical implementation, service delivery and resolution of problems rather than presenting the conceptual framework. There are detailed case studies in healthcare (Chang, 2014 a) and finance (Chang, 2014 b) to explain the process of transforming theory into practice, since service delivery with real users in place was a priority. However, there is a lack of demonstrations on security (despite of their three workshop papers), which is an important aspect of Cloud Computing service to ensure all services are well-protected.

In other words, the current version of CCAF needs revision by updating the security guidelines and business context. The emphasis should be as follows. First, how to make theory into practice. Several security papers have emphasized very much on the theoretical development and there is a lack of details describing how to reproduce similar results and replicate the success of delivering security services. Second, security technologies, measures and policies should be easily integrated with the existing practices. Third, the business context will be emphasized, since the improved framework should be adopted by industry and businesses that aim for long-term benefits such as cost reduction, business opportunities, profitability, improvement in efficiency and customer satisfaction as discussed in Section 1. The development of security and business solutions should be clear and easy to adopt. Thus, these three main factors drive us into the development of Cloud Computing Adoption Framework Update 1 (CCAF 1.1). Proof-of-concepts will be demonstrated to support our proposed CCAF 1.1.

1.2 The Integrated Data Center for Everything as a Service

To blend and manage security and business solution into CCAF 1.1, strategic directions have to be set and deployed to ensure that all future and emerging services, or Everything as a Service (EaaS), can be successfully delivered. EaaS includes design, deployment and guideline for Infrastructure, Platform and Software as a Service. Other value

added services such as Business Process, Security and Consulting as a Service are also part of EaaS.

The rationale for the IBM's approach is to start with the next-generation data center. The aim is to consolidate all resources and improve the percentage of resource utilization. This can ensure that Data center can be fully used and not to waste much energy and space. Similarly, platform and software as a service can be built on top of a smart data center into an integrated system model (Li, 2014). The integration starts from the infrastructure as a service level where the server, storage, networks and system management software is pre-integrated prior to shipping to the data center. The scope of the pre-integration varies from single rack systems within a traditional data center to a full size datacenter-in-a-box container. All the hardware integration is important for EaaS, since it will take much less time to send the network from one end to the other within the data center. Performance and response time can be enhanced significantly. The downtime caused by the bottleneck of network and storage will be less likely to happen, since the integrated data center can provide intelligent systems to warn the system manager, reassign extra demands to under-utilized data centers and ensure all resources can be smartly utilized.

2. SECURITY UPDATES

This section describes security update for Cloud Computing Adoption Framework Update 1 (CCAF 1.1). Topics include cyber attacks overview and recent attack methods, which help revise the counter-attack and remedy actions or CCAF 1.1.

2.1 Security Overview

The data leakage incidents due to various reasons, as reported by the DataLossDB.org have been on the rise in recent years according to DataLossDB.org survey (2013). The rapid jump from 2005 to 2006 is due to various disclosure legislations. The term Threat can be divided into *Internal Threats*, and *External Threats*. The former is originated from authorized users compromising and exploiting internal systems, while the latter are from external attackers. In both cases, the attackers seek to compromise systems by accessing data, gaining control of systems and applications, or disrupting their operation. Based on the technical report (Li, 2014), 57% of the loss incidents are due to external attacks while 36% are due to insiders as of the end of July, 2013 based on the IBM survey.

To expand this area further, the *Internal Threats* can be further subdivided into threats from *Insiders with Malicious Intent*, and threats from *Unintentional Insiders*. The risk posed by a malicious insider intents on compromising internal systems must be mitigated by a range of security measures, including background checks, restricting access, physical monitoring, platform integrity monitoring and controls on desktop applications and operations as well as profiling and auditing of user interactions with key applications and data. With the threat landscape so defined, the primary threats that require mitigation include:

1. *Malcode*: This threat comes from programs, scripts, or macros that are malicious in nature and can execute on user machines. This category of threats is often subdivided into *viruses* and *Trojans*. A *virus* is code that is attached to or contained within a legitimate application or document. A *Trojan* is a program that has an externally visible purpose and behavior, but also has covert, malicious behavior that is invisible to the user. A variety of stealth technologies can be deployed to keep malcode installed without detection (e.g. root kits). Self-propagating code is also often referred to as a *Worm*.

2. *Vulnerabilities*: These are deficiencies in legitimate code running on internal computer systems. If an attacker can interact with a vulnerable system that is internal to a network, or provide data to it, then it is possible for the attacker to exploit such a vulnerability to compromise the system. As with malcode, the vulnerability threat has several sub-categories, for example, SQL injection and Cross Site Scripting vulnerabilities (XSS). The most devastating types of vulnerabilities are those designated as *Remote Code Execution*. These vulnerabilities can allow code execution natively on the computer containing the vulnerable code (for example, using browsers or browser plug-ins). During the week of April 6, 2009 alone, US-CERT reported 142 vulnerabilities rated high or medium value.

3. *Data Loss and Leakage*: This threat often comes from insiders unintentionally transferring restricted information to external systems. This can also result from malcode installed on users' machines. Detecting and preventing the transfer of sensitive information from within an

organization to an unauthorized external site is the focus. Data loss can also result from the intentional actions of insiders focused on stealing valuable information.

4. *Denial of Service* (DOS): This threat comes from external users or systems attacking a targeted system's infrastructure with the intent to disrupt its operation to the degree necessary to degrade or disable its ability to serve its users. There are various forms of DOS attacks: one is the vulnerability DOS; some are vulnerabilities that might not be exploitable to gain Remote Code Execution, but can be exploited to crash the system. More common are DOS disruptions that arise from a high volume of spurious (attacker) traffic that overwhelms a network or host computer. If an attacker can construct a sequence of packets that overloads a host computer's capacity, then a flood of these packets can cause a denial of service. *Bandwidth DOS* attacks also seek to exhaust the network capacity by flooding the network with traffic. Often these attacks are coordinated to originate from thousands of different host computers (Distributed Denial of Service Attack) that have been compromised with botnet malcode installed covertly. These threats are unleashed by attackers with increasing creativity, for example: malcode often communicates over encrypted sessions; Javascript is often used to evade Intrusion Prevention Systems by obfuscating exploits; low bandwidth data leakage is difficult to detect and stop on the wire.

5. *Web Vandalism and Propaganda*: Attacks that deface Web pages, or spread political messages to anyone with access to the Internet.

6. *Botnets*: Collections of compromised computers (i.e. zombie computers) running programs, such as worms, Trojan horses, or backdoors, under a common command and control structure.

7. *Equipment Disruption*: This is the threat of physical tampering or destruction of computing equipment. For example, military activities that use computers and satellites for coordination are at risk from this type of physical attack.

8. *Critical Infrastructure Attack*: National electric power, water, fuel, communications, commercial and transportation systems are all vulnerable to cyber attacks.

2.2 Recent Attack Methods

Understanding the recent attack methods will help revise the guidelines and software fixes for CCAF 1.1. There is a list of cyber security incidents between February and Augst of 2011 compiled by X-Force of IBM, which include Amazon's loss of data in 2011 and 2012, and the problems with Elastic Load Balancing services in 2013 and RSA's hacked data and services (Li, 2014). It is apparent that the frequency and the size of the impact monotonically increased during this period.

Among all these incidents, the most severe incident is the attack on RSA during March 2011. This incident involves what is known as ***Five-layered of Advanced Persistent Threat*** (APT), and often includes the following five phases over an extended period of time:

1. **Social Engineering**: Initially, spear phishing emails were sent over a two-day period to small groups of employees with RSA. The email subject line read *2011 Recruitment Plan*, was from beyond.com – an HR partner firm of RSA. The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability. One of the RSA employees clicked the attachment from junk mail.
2. **Back Door**: The malware installed a customized remote administration tool known as Poison Ivy RAT to allow external control of the PC or server, and set up the tool in a reverse-connect mode
3. **Moving Laterally**: The malware first harvested access credentials from the compromised users (user, domain admin, and service accounts), then performed privilege escalation on non-administrative users in the targeted systems, and then moved on to gain access to key high value targets.
4. **Data Gathering**: Attacker behind the malware in the RSA case established access to staging servers at key aggregation points.
5. **Exfiltrate**: The attacker then used FTP to transfer many password-protected RAR files from the RSA file server to an outside staging server on an external, compromised machine at a hosting provider. Once the transfer completed, the footprints were wiped clean making it impossible to trace back to the attacker(s).

3 OUR PROPOSED SOLUTION

This section describes our proposal for designing and deploying the security solutions. The approach is to use a framework that can integrate different aspects of security. We propose the "Fine Grained Security Model" (FGSM), which offers the multi-layered security layer for Cloud Computing services. Since each type of security has its strengths and weaknesses, the combination of different security solutions can enhance the strengths and reduce the weakness if only one single solution is deployed.

3.1 The Overview

Before introducing the details of our updated framework, each element of the CCAF security is described as follows.

Identification is a basic and the first process of establishing and distinguishing amongst person/user & admin ids, a program/process/another computer ids, and data connections and communications.

Privacy is the key to maintaining the success of cloud computing and its impact on sharing information for social networking and teamwork on a specific project. This can be maintained by allowing users to choose when and what they wish to share in addition to allowing encryption and decryption facilities when they need to protect specific information/data/media content.

Integrity is defined as a process of maintaining consistency of actions, communications, values, methods, measures, principles, expectations, and outcomes. Ethical values are important for cloud service providers to protect integrity of cloud user's data with honesty, truthfulness and accuracy at all time.

Durability is also known as, persistency of user actions and services in use should include sessions and multiple sessions.

The other important aspects are as follows.

Confidentiality, Privacy and Trust – These are well known basic attributes of digital security such as authentication and authorization of information as well protecting privacy and trust.

Cloud services security – This includes security on all its services such as SaaS, PaaS, and IaaS. This is the key area of attention needed for achieving cloud security.

Big data security – This category is again paramount to sustaining cloud technology. This includes protecting and recovering planning for cloud data and service centers. It is also important to secure data in transactions.

Physical protection of cloud assets – This category belongs to protecting cloud centers and its assets.

3.2 The Fined Grained Security Model

CCAF security software implementation is demonstrated by the use of the Fine-Grained Security Model (FGSM), which has layers of security mechanism to allow multi-layered protection. This can ensure reduction in the infections by trojans, virus, worms, and unsolicited hacking and denial of service attacks. Each layer has its own protection and is in charge of one or multiple duties in the protection, preventive measurement and quarantine action presented in Figure 1.

All the features in FGSM include access control, intrusion detection system (IDS) and intrusion prevention system (IPS), this fine-grained security framework introduced fine-grained perimeter defense. The layer description is as follows.

- The first layer of defense is **Access Control and firewall** to allow restricted members to access.
- The second layer consists of the **IDS and IPS**. The aim is to detect attack, intrusion and penetration, and also provide up-to-date technologies to prevent attacks such as DoS, anti-spoofing, port scanning, known vulnerabilities, pattern-based attacks, parameter tampering, cross site scripting, SQL injection and cookie poisoning. The identity management is enforced to ensure that right level of access is only granted to the right person.
- The third layer, being an innovative approach, **Encryption**, enforces top down policy based security management; integrity management. This feature monitors and provides early warning as soon as the behavior of the fine-grained entity starts to behave abnormally; and end-to-end continuous assurance which includes the investigation and remediation after an abnormality is detected.

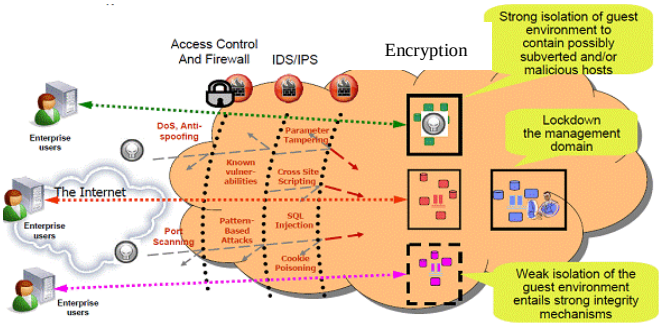

Figure 1: The Fine-Grained Security Model offered by CCAF

3.3 Technologies behind FGSM

This section describes the technologies behind FGSM, which uses XACML 3.0 (Extensible Access Control Markup Language), an XML-schema to define the which ports for secure communications with respect to the IP addresses. All the ports support secure ssh and ftp. XACML 3.0 has followed the industry standard to define the access control policy and how to access requests based on rules supported by the policies (Parducci et al., 2013). Our scripts have been carefully reviewed and tested under the testing and live environments. Additionally, the use of the integrated hardware and software technologies ensure a better protection for users and organizations. The description for each security layer is as follows.

In the first layer, firewall, we adopt the combination of Cisco and XACML technologies. Cisco routers and networking infrastructure allow us to set the firewall and monitor any abnormal activities. The use of XACML can enforce the strength of the security and minimize any errors, which include acknowledging the malicious (but well-hidden) code as the safe code.

In the second layer, identity management defines the type of users and their privilege and permission. These include the followings:

- Users: who can encrypt each key from his block and his own key. This step is to ensure that all the data that users access and store are protected in the Cloud.
- CCAF server: Three functions are as follows. First, it can authenticate users during the storage and retrieval process. Second, it offers access control for users. Third, it encrypts data between users and the Cloud.
- Security Manager (SM): This stores metadata which includes block signatures, encrypted keys and process identity management check. SM also checks whether a user is authorized to retrieve a file that he/she has requested, which offers an additional access control.

In the third layer, it adopts convergent encryption, which aims to consolidate all the files to be encrypted for storage. There are advanced but easy-to-use cryptography algorithms deployed. We can minimize the de-duplication of the same files and can monitor the changes and updates of encrypted files. This can ensure all the data coming in and out of the CCAF server to be protected to reduce the possibility that messages to be hijacked.

3.4 Isolation and quarantine

The FGSM also provides the detection and intrusion systems which record the typical behaviors of the trojans, viruses and worms. When the identified trojans, viruses and malicious code are found, they are isolated and sent to the quarantine area immediately. The strong isolation and integrity management are jointly used to protect user safety. Strong isolation is used to detect vulnerabilities in any of the cloud services, including the block of unauthorized IPs and attack points/ports. Quarantine is the next step to enforce security. It first backups the data safely and then attempts to quarantine infected data. If a quarantine action is unsuccessful, it informs the system architect. The files can be kept under “quarantine area” or chosen to be deleted.

3.5 Resilient Computing

As discussed in Section 1, the intelligent Data Center will integrate all hardware infrastructure and applications supporting the hardware. The benefit is to provide a better access, integration and performance than the current Data Center deployment. With regard to this, IBM has proposed the Resilient Computing which integrates Cloud Computing hardware and software with security. The updated CCAF framework will be essential to IBM Resilient Computing development.

4 CONCLUSION AND FUTRUE WORK

This paper provides a strategic overview and direction for the improved Cloud Computing Adoption Framework update 1 (CCAF 1.1), in

which the emphasis is on the update on security policy, technologies and techniques used. The security recommendation and updates can help organizations building and offering better protected services. Different types of technologies and techniques have been discussed. The proposed Fine Grained Security Model (FGSM) offers multi-layered security and is a suitable solution in the deployment of Cloud Computing services, since each single solution has its weakness. The core technology in each layer of FGSM have been described and justified, which includes the firewall, the identity management and convergent encryption. The combination of three main security solutions in FGSM can enforce security service.

The FGSM prototype will be developed and then thoroughly tested in the laboratory conditions. We plan to use ethical hacking and penetration testing approached to test the robustness of our FGSM security. This will be fully implemented in our CCAF and eventually the development of Resilient Computing. If the results are positively in favor of our prototype and security strategy, we will update our recommendation, results and guidelines, which will be developed into CCAF Version 2.

REFERENCES

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M., 2010. A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58.

Chang, V., 2014 a. Cloud Computing for brain segmentation – a perspective from the technology and evaluations. International Journal of Big Data Intelligence, 1, (4), 192-204.

Chang, V., 2014 b. The business intelligence as a service in the cloud. *Future Generation Computer Systems*, *37*, 512-534.

Chang, V., 2015. A Proposed Cloud Computing Business Framework, ISBNs: 9781634820172 (print), Nova Science Publisher.

Chang, V., Li, C. S., De Roure, D., Wills, G., Walters, R. J., & Chee, C., 2012. The financial clouds review. Cloud Computing Advancements in Design, Implementation, and Technologies, 125.

Chang, V., Walters, R. J. & Wills, G., 2013 a. The development that leads to the Cloud Computing Business Framework. International Journal of Information Management, June, 33, (3), 524-538.

Chang, V., Walters, R. J. & Wills, G., 2013 b. Cloud Storage and Bioinformatics in a private cloud deployment: Lessons for Data Intensive research. In, Cloud Computing and Service Science, Springer Lecture Notes Series, Springer Book.

DataLossDB.org survey, 2013, accessible on http://datalossdb.org/us_states in 2013.

IBM, 2010. Defining a framework for cloud adoption, technical report.

Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I., 2010, July. Cloud migration: A case study of migrating an enterprise it system to iaas. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on (pp. 450-457). IEEE.

Li, C. S, 2014. Resilient Computing, technical report, IBM.

Low, C., Chen, Y., & Wu, M., 2011. Understanding the determinants of cloud computing adoption. *Industrial management & data systems*, *111*(7), 1006-1023.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A., 2011. Cloud computing—The business perspective. *Decision Support Systems*,*51*(1), 176-189.

Parducci, B., Lockhart, H., Levinson, R., 2013. OASIS eXtensible Access Control Markup Language (XACML) TC, technical report, accessible on https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

Ramachandran, M., & Chang, V. 2014. Financial Software as a Service–A Paradigm for Risk Modelling and Analytics. *International Journal of Organizational and Collective Intelligence* 4(3).

Velte, T., Velte, A., & Elsenpeter, R., 2009. *Cloud computing, a practical approach*. McGraw-Hill, Inc.

Weinhardt, C., Anandasivam, D. I. W. A., Blau, B., Borissov, D. I. N., Meinl, D. M. T., Michalk, D. I. W. W., & Stößer, J., 2009. Cloud computing–a classification, business models, and research directions. Business & Information Systems Engineering, 1(5), 391-399.